Вх. № РД-08-74/30.01.2019 г. Тема: ” Синтез на алгоритми за защита на данни

Финансиране **2206.28**лв.

ЕКИП

Ръководител на проекта:	**Преподавател/докторант/ студент**
1. Проф. д.н. Борислав Панайотов Стоянов	**преподавател**
Членове на колектива:	
2. Гл. ас. д-р Валентина Спасова Дянкова	преподавател
3. Гл. ас. д-р Бисерка Бончева Йовчева	преподавател
4. Преп. д-р Михаела Димитрова Тодорова	преподавател/докторант до 09.09.2019 г.
5. Преп. Цветелина Росенова Иванова	докторант
6. Александър Симеонов Куцаров	студент
7. Синан Айдън Осман	студент
8. Ерджан Юксел Ахмед	студент
9. Гарегин Мелик Борборян	студент

ОСНОВНИ РЕЗУЛТАТИ

Извършени са изследвания по софтуерно моделиране и криптографско изследване на предложения от Шнайер редуващ стъпков генератор на псевдослучайни двоични числа. Кодирането е направено на езика за програмиране CPP. За начални стойности на модела са използвани взаимно простите числа от 984059 до 2305883.

Статистическото тестване на псевдослучайния генератор е осъществено с приложния софтуер NIST test suite. Получените отлични изходни резултати са сравними с други NIST данни от шест подобни генератори.

Може да се направи аргументиран извод, че данните от моделирането показват, че изследвания редуващ стъпков генератор има подходящи характеристики за включване в различни криптографски примитиви.

ПУБЛИКАЦИИ ПО ПРОЕКТА

1. Stoyanov, B. (2019) One Modification of the Alternating Step Generator, Proceedings of the National Conference on "Education and Research in the Information Society", Plovdiv, Bulgaria, May, 2019, 112-116. (Google Scholar, Национален референтен списък (НРС))